

Common Elements of Risk

Christopher J. Alberts

April 2006

Acquisition Support Program

Unlimited distribution subject to the copyright.

Technical Note
CMU/SEI-2006-TN-014

This work is sponsored by the U.S. Department of Defense.

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2006 Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (<http://www.sei.cmu.edu/publications/pubweb.html>).

Contents

Acknowledgements	vii
Abstract.....	ix
1 Introduction	1
1.1 Background.....	1
1.2 Objectives, Audience, and Structure.....	2
2 Deconstructing Risk.....	3
2.1 Different Types of Risk.....	3
2.2 Operational Risk	4
2.3 The Core Elements of Risk.....	6
2.4 Strategic Risk.....	6
2.5 Operational Risk	7
3 Sources of Operational Risk.....	10
3.1 Work-Process Elements	10
3.1.1 Mission.....	11
3.1.2 Process Design.....	11
3.1.3 Activity Management.....	12
3.1.4 Operational Environment	13
3.1.5 Event Management.....	14
3.2 Categories of Operational Threat	14
3.2.1 Mission Threats.....	15
3.2.2 Design Threats.....	15
3.2.3 Activity Threats	16
3.2.4 Environment Threats.....	16
3.2.5 Event Threats.....	17
3.3 Elements of Operational Threat.....	18
4 Potential Applications	20
4.1 Expressing Risk	20
4.2 Mitigating Risk	21

5	Conclusion	22
	Feedback	24
	References.....	25

List of Figures

Figure 1: Speculative and Hazard Risks.....	4
Figure 2: The Four Elements of Risk.....	6
Figure 3: The Basic Elements of Operational Risk.....	7
Figure 4: Controls and Operational Risk	8
Figure 5: Threat and Operational Risk	9
Figure 6: Work Process with Four Activities	10
Figure 7: Structural Elements of a Work Process.....	12
Figure 8: Activity Management	13
Figure 9: Operational Environment.....	13
Figure 10: Event Management	14

List of Tables

Table 1: Elements of Operational Threats.....	18
---	----

Acknowledgements

This technical note is jointly sponsored by the Acquisition Support and the Networked Systems Survivability Programs of the Carnegie Mellon[®] Software Engineering Institute (SEI).

I would like to acknowledge the following individuals for reviewing this report and providing comments: Julia Allen, Audrey Dorofee, and Eileen Forrester. I would also like to acknowledge Susan Kushner for editing the document.

[®] Carnegie Mellon is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Abstract

Traditionally, responsibility for completing a mission and the resources needed to pursue it aligned with organizational boundaries. However, key drivers in the business environment, such as the globalization of business and the fast pace of technological change, have resulted in increased outsourcing and partnering among organizations. It is now common for multiple organizations to work collaboratively in pursuit of a single mission, which creates a degree of programmatic and process complexity that can be difficult to manage effectively. In today's business environment, management and staff must be able to deal with intricate and unclear interrelationships and dependencies among technologies, data, tasks, activities, processes, and people. Mission success in these complex environments requires people to sort through the inherent complexity when making important decisions. Effective risk management that is based on a solid conceptual foundation is an essential part of this decision-making process. This technical note begins to define this foundation by identifying the basic elements of risk and exploring how these elements can affect the potential for mission success.

1 Introduction

Responsibility for completing a mission and the resources needed to pursue it traditionally aligned with organizational boundaries. However, key drivers in the business environment, such as the globalization of business and the fast pace of technological change, have led to increased outsourcing and partnering among organizations. It is now common for multiple organizations to work collaboratively in pursuit of a single mission, which creates a degree of programmatic and process complexity that is difficult to effectively manage. Mission success in these complex environments requires a collaborative management approach that effectively coordinates task execution, decision making, and risk management activities among all participating groups.

1.1 Background

About three years ago, the Carnegie Mellon[®] Software Engineering Institute (SEI) chartered a team to research approaches for managing risk in complex environments. When setting the scope of this work, we focused on one particular type of operational complexity: distributed work processes. The term *work process*, as used in this document, refers to a collection of interrelated work tasks that achieves a specific result [Sharp 01].¹ A *distributed work process* is one for which management control is shared by multiple managers that often reside in different organizations.

Over the past several years, outsourcing and collaboration have becoming increasingly popular, which has made distributed work processes commonplace. The paradigm of having a single manager with absolute responsibility for an entire work process is becoming obsolete. It is being replaced by a collaborative model where management responsibility for a process is shared by several managers, each overseeing a part of the overall process. In addition, work-process activities are no longer supported by dedicated, stand-alone technologies. Rather, interoperable, networked technologies now support work processes. Management and staff must now deal with interrelationships and dependencies among technologies, data, tasks, activities, processes, and people that were unimaginable just a few years ago. Not surprisingly, the complexity inherent in these distributed work processes beckons for new and innovative approaches for managing risk.

[®] Carnegie Mellon is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

¹ The literature uses several terms synonymously with work process, including business process, workflow, process, and operational process. All five terms are used interchangeably throughout this document.

The research currently being performed is intended to address the need for new and innovative risk management approaches that can be employed in a variety of settings, including (but not limited to)

- large, distributed software development programs
- Department of Defense supply chains
- distributed information-technology (IT) processes for configuring and maintaining an organization's computing infrastructure
- core business processes that are distributed across departments in a single organization, such as a patient-care process in a medical facility

While each of these examples possesses unique characteristics, all share a common conceptual basis—distributed work processes that by their very nature increase risk.

Our ultimate research goal is to develop a flexible suite of methods, tools, and techniques for managing risk in distributed work processes, such as those listed above. Establishing a solid conceptual foundation in the area of risk management is essential to achieving this goal. As a result, we decided to begin our work by answering the following fundamental questions:

- What constitutes risk?
- What factors put operational missions at risk?

This technical note explores these two important questions. The research presented in this document is a work in progress; it presents concepts developed in support of our research in the area of mission assurance. Over time, we will refine and enhance this information as research progresses. Future publications will reflect any changes or updates to the concepts and philosophies presented in this report. The purpose for publishing these interim results is to solicit feedback from the community and incorporate that input into future research.

1.2 Objectives, Audience, and Structure

The key objectives of this technical note are to (1) define the basic elements of risk and (2) explore how these elements affect work processes. This technical note is written for people who have experience assessing and managing risk in operational settings. It is divided into four sections. This introduction serves as the first section; it provides background about the research contained in this document. Section 2, “Deconstructing Risk,” examines the core elements of risk and discusses how they apply to strategic and operational risk. Key causes of operational risk are featured in Section 3, “Sources of Operational Risk.” This section examines what conditions can put core business processes at risk. Section 4, “Potential Applications,” explores how the ideas in this technical note might be applied to selected risk management topics. Finally, Section 5, “Conclusion,” completes the report by summarizing the history of the research described in this report and illustrating how the research findings have influenced SEI work in the area of mission assurance.

2 Deconstructing Risk

To understand the nature of risk, we must begin with its definition. Although there are many variations in how risk is defined, the following definition succinctly captures its essence: risk is the possibility of suffering loss [Dorofee 96]. This definition includes two key aspects of risk: (1) some *loss* must be possible and (2) there must be *uncertainty* associated with that loss. One additional condition is necessary for risk to be present: a *choice* about how to address it.² These three conditions form the basic underpinnings of risk and provide a basis for a more in-depth examination of it.

2.1 Different Types of Risk³

The term *risk* is used universally, but different audiences often attach slightly different meanings to it [Kloman 90]. For example, the way in which risk relates to opportunity depends on the context in which risk is being viewed. Sometimes a situation presents both an opportunity for gain as well as the potential for loss. In other instances, there is no opportunity for gain, only the potential for loss. Risk can thus be further subdivided into two types: speculative risks and hazard risks [Young 01].

Figure 1 illustrates the differences between these two categories. With speculative risk you can realize a gain, improving your current situation relative to the status quo. At the same time, you have the potential to experience a loss, making you worse off than you are at present. Gambling is an example of taking a speculative risk. When you place a bet, you must weigh the possibility of gaining additional money against the prospect of losing what you wagered. In this example, your overall objective is to increase your wealth, and you are willing to put money at risk to provide yourself an opportunity to make money.

In contrast, hazard risk only has potential losses associated with it and provides no opportunity to improve upon the current situation. For example, consider how security can be viewed as a hazard risk. Imagine that you are concerned about protecting valuables that are stored in your home. Your main objective in this example is to ensure that none of the valuables in your residence is removed without your knowledge and permission. After evaluating how well your valuables are protected, you might decide to install a security system in your residence to make it more difficult for a thief to break in and steal your valuables. Notice that the objective in this example, by definition, restricts the focus of risk

² Most definitions of risk explicitly reference loss and uncertainty. The third aspect of risk, choice, is usually only implied.

³ Much of the material contained in Section 2.1 was originally presented in the technical note *Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments* (CMU/SEI-2005-TN-032) [Alberts 05].

on the potential for loss. In the most favorable of circumstances, you only keep what you already possess. There is no potential for gain.

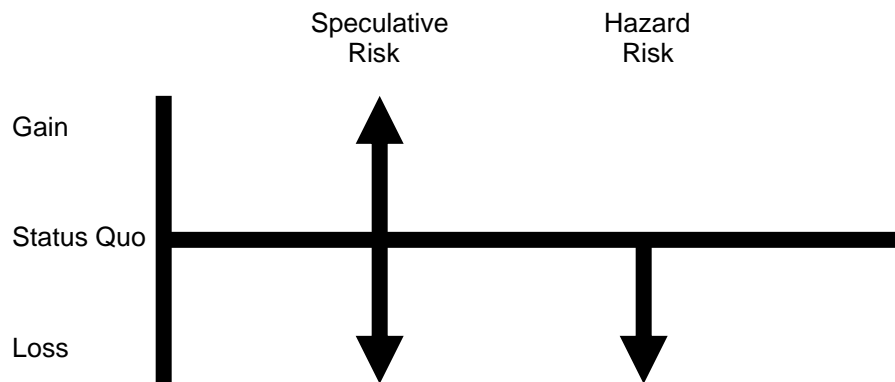


Figure 1: Speculative and Hazard Risks

Now consider another example involving security. In this instance, you would like to gain peace of mind by preventing unsavory characters from gaining entrance to your house. Your objective to feel more secure defines the context in which you view risk. After analyzing the situation, you might decide to install a security system in your residence to make it more difficult for someone to break in. You might reason that the added security will likely help you feel more secure and likely help you gain the peace of mind you seek. In this example, you are willing to invest money in a security system to provide yourself an opportunity to feel more secure. The security risk in this example is speculative because it balances your tolerance for risk (i.e., the amount of money you are willing to invest in a security system) with your desire to realize an opportunity (i.e., gaining peace of mind).

A risk is thus not classified as speculative or hazard based on its type, but upon the context in which it is viewed. The notion of explicitly establishing the context in which you analyze and manage risk is vitally important to ensure that you make appropriate choices. The role of context with respect to risk is discussed further in Section 2.3 in which we present the core elements of risk.

2.2 Operational Risk

Managers in every organization deal with risk on many levels. Upper management most often focuses on the speculative nature of risk. Management balances the risk of investing organizational capital against the potential return on that investment and strategically manages risk across the organization's portfolio of activities and investments. However, at the operational levels of an organization, staff and management are more typically focused on managing a form of hazard risk called operational risk. As staff and management execute work processes, operational risks begin to emerge. Deficiencies inherent in processes can

lead to inefficiencies and problems during operations, which can adversely affect the organization's chances for success.

Unfortunately, there is no universally accepted definition of the term *operational risk*. The Basel Committee on Banking Supervision published a capital adequacy framework commonly known as Basel II that includes a definition of operational risk commonly used in the financial community. Operational risk, as defined in the Basel II framework, is “the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events” [BIS 04].

The Basel II definition of operational risk focuses on risk stemming from the *execution* of a work process. However, it does not account for a second, equally important aspect of risk that can occur during operations: the risk associated with the *expected outcome* of a process (i.e., its mission). For example, in software development, there can be considerable risk associated with the product being developed (i.e., the outcome, or mission, of the development process). If the development of a software-intensive system is an *unprecedented* effort, considerable risk is inherent in the system being developed. Because an unprecedented system, by definition, has not been developed before, management and staff must base their plans on assumptions rather than experience and data. As a result, there is a very real possibility that the system will not be developed within its quality, schedule, and cost parameters because key assumptions likely will not accurately reflect the reality that unfolds. In fact, when developing an unprecedented system, little risk may be associated with the processes, people, systems, or external events (the key sources of operational risk according to Basel II), yet the mission could still be at considerable risk due to the uncertain nature of the development effort. Notice that the risk embedded within a mission is beyond the scope of the Basel II definition of operational risk. As a result, a broader definition of operational risk is needed.⁴

The following definition of operational risk is used throughout this document: *operational risk is the potential failure to achieve mission objectives*. This definition includes loss (failure to achieve mission objectives) and uncertainty (possibility that the failure might or might not occur). At the same time, it is sufficiently general to be applied in a variety of diverse domains.

To summarize, although there are many different forms of risk (e.g., business, operational, project, and security risks) all share the same conceptual basis. At the same time, there can be significant differences among the tangible characteristics of various types of risk based on the context in which it is viewed. For example, a speculative risk, like business risk, has unique qualities that differentiate it from a hazard risk, such as operational risk. The speculative nature of business risk allows for both gain and loss, while operational risk offers no opportunity for gain.

⁴ A second solution is to define another type of risk, rather than expand the definition of operational risk. This alternative is addressed in Section 5.

So far, our discussion has focused on the conceptual aspects of risk. The next section explores risk's more tangible aspects by defining its core elements.

2.3 The Core Elements of Risk

All forms of risk, whether they are classified as speculative or hazard risks, comprise common elements. This notion is illustrated in Figure 2, which highlights the following four basic components of risk: (1) context, (2) action, (3) conditions, and (4) consequences.

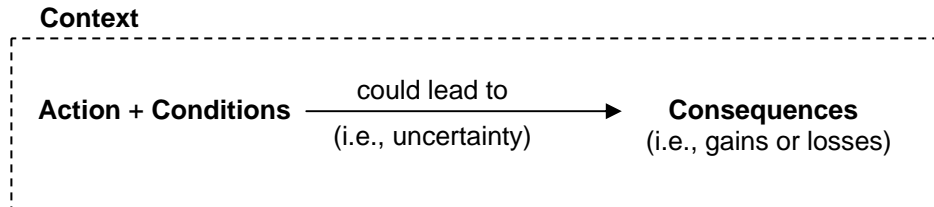


Figure 2: The Four Elements of Risk

Context is the background, situation, or environment in which risk is being viewed and defines which actions and conditions are relevant to that situation. In other words, the context provides the lens through which all consequences are evaluated. Without setting an appropriate context, you cannot definitively determine which actions, conditions, and consequences to include in risk analysis and management activities. Context thus forms the foundation for all subsequent risk management activities.

After the context is established, the remaining elements of risk can be appropriately considered. The *action* is the act or occurrence that triggers risk. It is the active component of risk and must be combined with one or more specific conditions for risk to be present. All forms of risk are triggered by an action; without the action, there is no possibility of risk.

Whereas the action is the active component of risk, *conditions* constitute risk's passive element. They define the current state or the set of circumstances that can lead to risk. Conditions, when combined with a specific triggering action, can produce a set of consequences, or outcomes. *Consequences*, the final element of risk, are the potential results or effects of an action in combination with a specific condition(s).

When risk is present there is, by definition, a potential for loss. Depending on the circumstances, there might also be a potential for gain (i.e., speculative risk). The next two subsections examine the four elements of risk in relation to strategic and operational risk.

2.4 Strategic Risk

Strategic risk is the risk a company takes to fulfill its business objectives. Implicit in this definition is the potential for both gain and loss, which makes strategic risk speculative in

nature. Consider how risk's four elements apply to strategic risk. For example, think about a situation where senior management in a financial institution is thinking about entering a new market, such as providing online banking services. As it works through its decision-making process, management must examine the potential opportunities and losses associated with that market.

The *context* in this particular example is the market for online banking services. All actions, conditions, and consequences must be viewed within this particular context. *Actions* in this example are the range of strategic options being considered. Management has a number of options it can pursue, including the following four: (1) decide to enter the market immediately, (2) hedge bets by offering a few trial services, (3) do nothing now, but reserve the right to play later, or (4) decide not to enter the market. *Conditions* in this example include the current trends and uncertainties related to online banking services, such as the number of potential customers, what actions competitors might be taking, and the current core competencies of the company. The combination of each strategic action with current trends and uncertainties produces a range of *consequences*, or potential gains and losses for the company. Management considers the relative degree of opportunity and risk resulting from each strategic action. It selects the best option based on the tolerance for risk in conjunction with the desire to take advantage of the opportunity.

The four core elements of risk thus provide a useful means to break down and understand a strategic business risk. These elements are also useful when considering a hazard risk, such as operational risk.

2.5 Operational Risk

Recall that the following definition of operational risk is used in this document: operational risk is the potential failure to achieve mission objectives. Figure 3 illustrates how the four elements of risk translate to operational risk. The words in the figure reflect terminology commonly used when describing operational risk. Notice that the *mission* of a work process defines the context in which operational risk is viewed. Defining the mission is an essential first step for characterizing operational risk because it forms the basis for identifying, interpreting, and managing it. All other elements shown in Figure 3 are examined in relation to the mission of a work process.

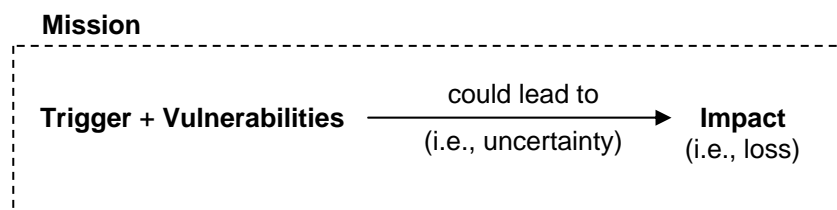


Figure 3: The Basic Elements of Operational Risk

The *trigger* is the act or event that, when combined with existing vulnerabilities, leads to a range of potential losses.⁵ *Vulnerabilities* are flaws or weaknesses that expose the process to those losses; *impacts* define the potential losses resulting from a realized risk. With operational risk, all losses are expressed in relation to the mission being pursued. Because it is a hazard risk, operational risk provides a potential for loss, but does not present a corresponding potential for gain.

One additional type of condition must be factored into the equation for operational risk: *controls*. Figure 4 shows the relationships between controls and triggers, vulnerabilities, and impacts. Controls are the circumstances that propel a process toward fulfilling its mission. They include the policies, procedures, practices, conditions, and organizational structures designed to provide reasonable assurance that a mission will be achieved and that undesired events will be prevented, detected, and corrected [ITGI 00].⁶

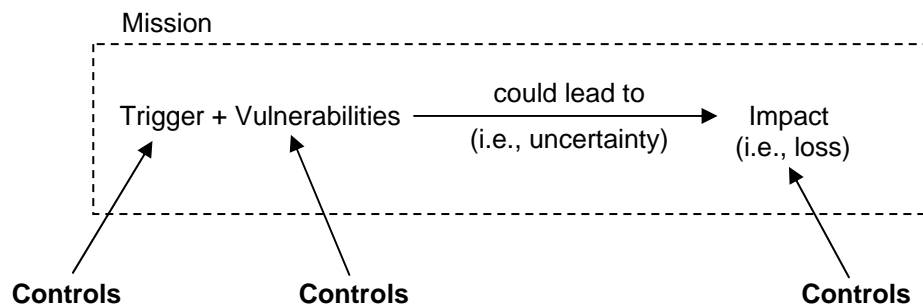


Figure 4: Controls and Operational Risk

Controls can help reduce risk by

- eliminating a triggering event
- monitoring for the occurrence of a trigger and implementing contingency plans when appropriate
- reducing vulnerability
- reducing potential impacts

Thus, a true measure of operational risk must include the influence of controls as well as the other four elements.

Finally, people commonly use the term *threat* when discussing operational risk. A threat is a circumstance or event that produces risk [Alberts 05]. As shown in Figure 5, a threat comprises a trigger and one or more vulnerabilities, because together these elements define

⁵ In security, the term *threat actor* is often used when describing what triggers a security risk (which is a subset of operational risk). The word *trigger* is used in this document to describe what initiates operational risk because it includes circumstances, acts, or events that are much broader than those considered in security risk.

⁶ This definition of *control* is derived from COBIT (Control Objectives for Information and Related Technology). COBIT is issued by the IT Governance Institute (<http://www.itgi.org>) and promoted by the Information Systems Audit and Control Association (<http://www.isaca.org>).

the circumstances that create the potential for harm or loss. Section 3 builds on the concept of threat by examining the five categories of threat that produce operational risk.

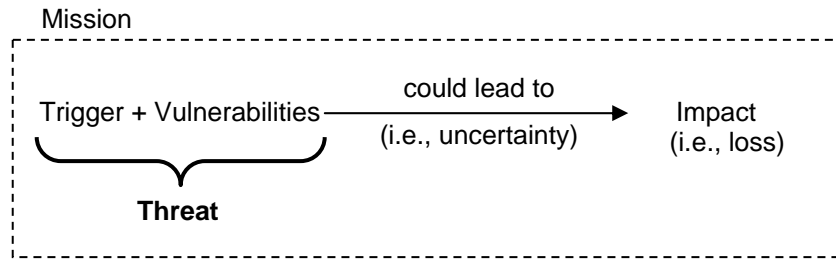


Figure 5: Threat and Operational Risk

3 Sources of Operational Risk

Analyzing the risk produced by various sources, or threats, is a foundational aspect of all risk management activities. With respect to operational risk, a key question that must be considered is: which threats lead to operational risk? Past research at the SEI examined operational risk in various settings, including software development [Dorofee 96, Williams 99], system acquisition [Gallagher 99], and operational security [Alberts 02]. Our research in these areas shows similarities and patterns among the types of threats that lead to operational risk. Recent SEI research examines these domains to identify a common structure for classifying sources of operational risk [Alberts 05]. The key to identifying this common structure is to decompose a work process into its core elements.

3.1 Work-Process Elements

Figure 6 depicts a generic work process and highlights the activities required to achieve its associated mission. Recall that a work process is a collection of interrelated work tasks that achieves a specific result and that its mission defines the set of the objectives pursued when executing that process.

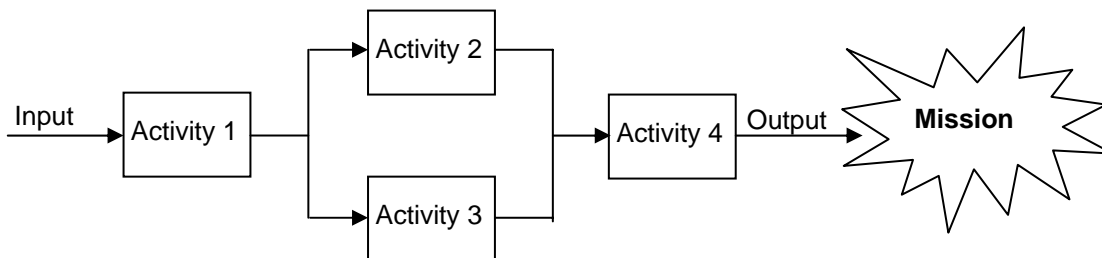


Figure 6: Work Process with Four Activities

The basic objective of the process depicted in Figure 6 is to transform the input into the desired output, forming the basis of the work-process mission. To achieve that mission, four activities must be executed in the order shown, while also adhering to any cost and schedule objectives. Process execution kicks off with Activity 1. After it is complete, its output feeds Activities 2 and 3, which are performed in parallel. When both of these activities are complete, their outputs are forwarded to Activity 4, the last in the sequence. Upon completion of Activity 4, the process is finished. If the activities have been performed correctly, the mission will have been successfully achieved.

A work process is more than a collection of activities, however. It is a complex *organizational system* that brings together a variety of diverse components, or assets. These

assets (people, technologies, equipment, facilities, information, procedures, and inputs) are organized in a specific way to achieve a particular mission. Process assets are not brought together in a random fashion when pursuing a mission. On the contrary, they are a set of interacting, interrelated, and interdependent parts that must function as a whole to accomplish the mission. Successful execution requires the process to be carefully structured and also effectively managed during operations. Thus, mission success (or lack of it) hinges on the structural and operational elements of a work process.

Structural elements capture the static aspects of a process: forming a plan of action and providing the foundation for process execution. There are two structural elements: mission and process design. By contrast, operational elements embody the dynamic aspects of a process, focusing on how the plan is implemented within the business environment. There are three operational elements: activity management, operational environment, and event management. All five structural and operational elements are examined in the subsections that follow.

3.1.1 Mission

The key objectives pursued when executing a work process are embodied in its mission, which typically comprises three distinct types of objectives: (1) product, (2) cost, and (3) schedule. Product objectives define the nature of the outputs produced by the process. (Product objectives are often referred to as technical objectives in the software development domain.) For example, if you are developing a software-intensive system, the product (i.e., technical) objectives define the performance characteristics of the system as well as other desired attributes, like reliability, safety, or security. Product objectives basically define parameters of success for the products you build or the services you provide and form the core objectives of a mission.

A mission could be solely defined by its product objectives. However, constraints must also be considered in relation to product objectives. Managers do not have infinite funds at their disposal, nor do they have an infinite amount of time in which to complete work tasks. As a result, cost and schedule objectives must be considered alongside the product objectives. These three types of objectives, when viewed together, typically define a basic mission. They specify what will be accomplished, the anticipated costs to complete all activities, and the time frame in which work will be completed. When appropriate, these objectives can be supplemented with other supporting objectives to ensure a complete picture of success.

3.1.2 Process Design

Whereas the mission defines what success looks like, the process design provides the roadmap for achieving that picture of success. The process design outlines the resources needed to complete a mission as well as all steps, decisions, and handoffs required to successfully execute a work process. A process design typically

- outlines people's roles and responsibilities
- ensures that activities are sequenced correctly
- identifies dependencies and interrelationships among the activities
- defines the timing requirements for each step in the process
- establishes practices and procedures that must be followed
- provides process artifacts, such as decision-making guidelines, templates, and written procedures
- defines technologies that are needed to support the process
- establishes measures and metrics for managing the process

The mission and process design, when viewed together, define a plan of action. You can think of them as forming the blueprint of the work process. They are important because they define a set of objectives as well as the path for achieving them. Figure 7 shows the relationship between the two structural elements of a work process.

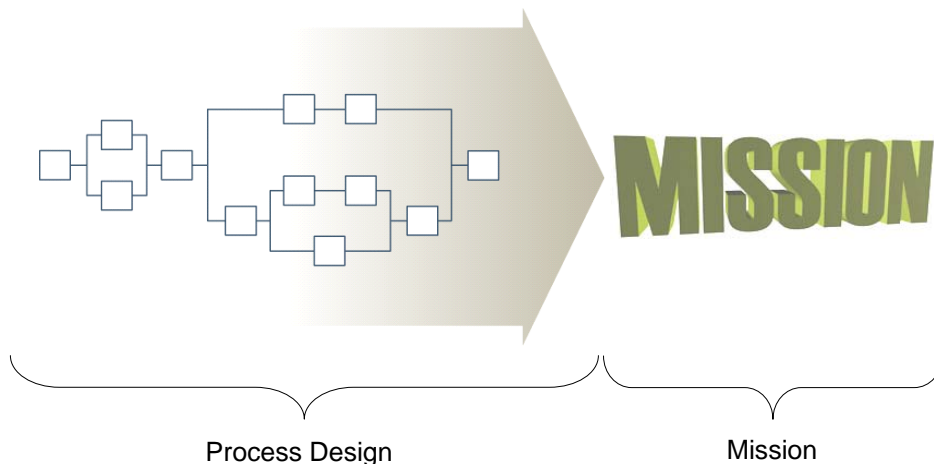


Figure 7: Structural Elements of a Work Process

3.1.3 Activity Management

Whereas the mission and process design provide the basis for process execution, activity management is focused on assembling, organizing, and overseeing the resources required to bring that plan to life. Examples of these resources include

- the people tasked with doing the work
- the technology and equipment that directly support work process execution
- the facilities in which the work will be completed
- software programs used to automate the process or to facilitate process execution

Figure 8 illustrates the notion that activity management makes a work process operational.

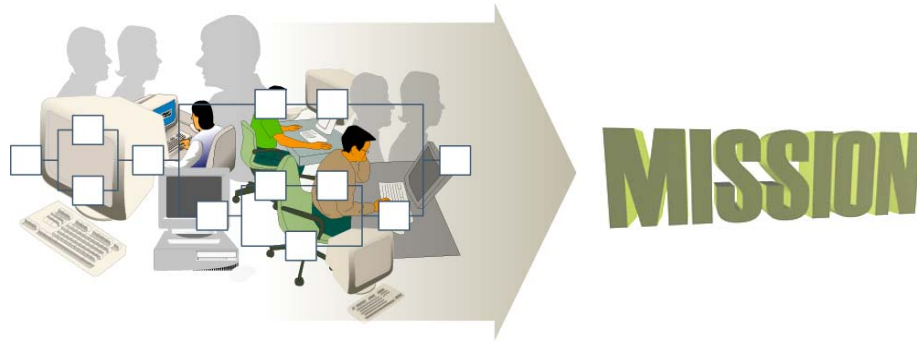


Figure 8: Activity Management

3.1.4 Operational Environment

Ideally, management and staff could focus exclusively on the tasks at hand and ignore how the broader operational environment affects process performance. However, the environment typically plays a role in how efficiently and effectively activities are performed. Management and staff must be aware of their surroundings and understand how environmental conditions might affect work tasks. The operational environment, which is the second operational element of work processes, includes an organization's structure, culture, and politics. It also includes any constraints that a work process inherits from the parent organization(s) in which it is executed or from the broader business environment. For example, these constraints can include restrictions imposed by laws and regulations as well as problems with services provided by third parties. Figure 9 adds the operational environment to the evolving picture of a work process.

Operational Environment

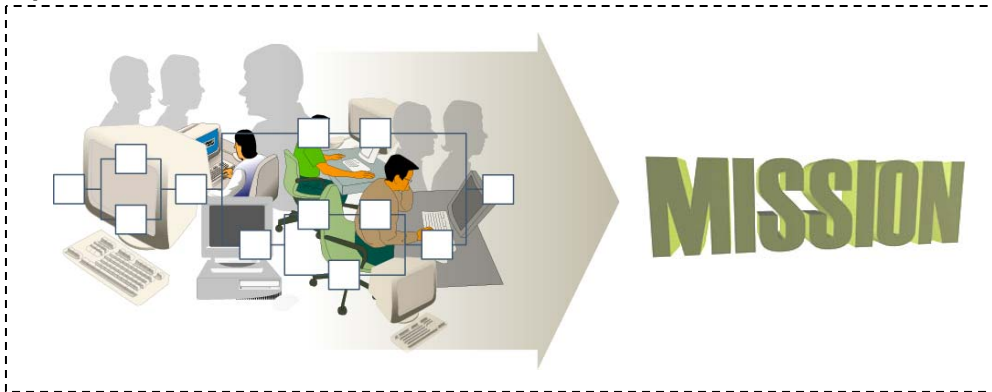


Figure 9: Operational Environment

3.1.5 Event Management

Thus far, we have focused on what it takes to plan and execute a process during normal, or expected, operational conditions. However, effective management must also take into account the possibility of problems resulting from unusual, or unexpected, circumstances (i.e., events). A process must be nimble enough to adapt to a range of possible situations or events. The final operational element, event management, highlights the ability to manage unpredictable events and change.

If the business environment were not subject to the effects of unexpected events and change, the previous four elements (mission, process design, activity management, and operational environment) would be sufficient to forecast the potential for success. However, the world is dynamic and unpredictable, which forces people to prepare for unusual or unexpected situations. Management and staff must be on alert for sudden events that can derail progress as well as for how incremental change can affect performance over time. Figure 10 adds the concept of events to the work-process diagram.

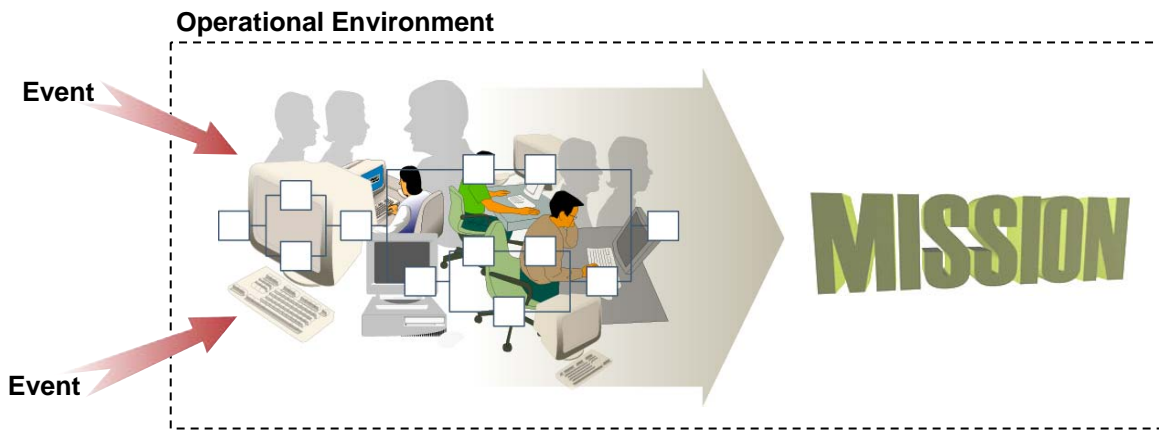


Figure 10: Event Management

As shown in Figure 10, the five work-process elements all play key roles in achieving a mission. They also provide the basis for exploring the range of threats that can cast doubt on the potential for mission success.

3.2 Categories of Operational Threat

Recall that a threat is a circumstance or event with the potential to cause harm or loss, which makes it the source of operational risk. A threat comprises two distinct elements: a trigger (the active component of threat) and one or more vulnerabilities (the passive component of threat). Five basic categories of operational threat uniquely map to the five work-process elements featured in Section 3.1. Each category is examined in the subsections that follow, beginning with mission threats.

3.2.1 Mission Threats

The mission is the cornerstone of a work process, defining what success looks like. If that definition is skewed or flawed, the entire system could be out of balance, producing unexpected or unwanted results. A *mission threat* is a fundamental flaw, or weaknesses, in the purpose and scope of a work process. It injects considerable vulnerability into the very foundation of a work process, exposing it to a substantial amount of operational risk. This vulnerability can manifest itself in a number of tangible ways, affecting all aspects of the process, from the layout and arrangement of activities to the resources assigned to those activities. Examples of mission threats include the following:⁷

- The core mission objectives are inherently risky.
- Funding is insufficient to complete the core mission objectives.
- Time is insufficient to complete the core mission objectives.
- Resources are insufficient to complete the core mission objectives.
- Mission objectives are unclear or unarticulated.
- The mission does not meet customer requirements and needs.
- Mission objectives are not defined and documented.
- Local missions are not aligned with the overarching mission.

3.2.2 Design Threats

While the mission describes the goal or objectives being pursued, the design of a process delineates the roadmap for achieving the mission. A *design threat* is an inherent weakness in the layout of a work process. It can have far-reaching consequences because it embeds risk within the structure of a process. Common design threats include

- The process is not defined and documented.
- The process is overly complex or inefficient.
 - Unnecessary tasks are performed.
 - There are bottlenecks.
- The process does not conform to accepted policy and practice.
- Procedures for performing tasks are not defined and documented.
- Roles and responsibilities are not defined and documented.
- Quality assurance is not built into the process.
- Supporting technologies are not designed to facilitate process execution.
- Facilities (i.e., physical layout of work space and equipment) do not support efficient execution of the process.

⁷ The list of threats for each of the five categories of operational threat provides examples of threats in that category. It is not a comprehensive compilation of all possible threats.

- Performance measures or metrics for managing the process are not defined.

3.2.3 Activity Threats

Activity management builds upon the structural elements of a work process by assembling, organizing, and overseeing the resources needed to execute that plan. An *activity threat* is a flaw, or weaknesses, arising from the manner in which activities are managed and performed. A variety of circumstances can produce this type of threat, ranging from people's actions to unreliable performance of support technologies. In essence, activity threats occur when actual performance deviates from what was planned or anticipated (e.g., as outlined in the design). Potential activity threats include the following:

- Staff members do not possess the necessary knowledge, skills, and abilities to perform expected tasks.
- Staffing levels are insufficient to complete all assigned tasks.
- Staff members do not receive adequate training related to domain knowledge.
- Staff members do not receive adequate training related to process execution.
- The staff does not efficiently execute the process as defined.
- Inputs to an activity are not accurate and complete when received (i.e., they contain defects).
- Inputs to an activity are not received on time.
- Management does not facilitate completion of the process.
- Risk is not managed effectively.
- Problems are not resolved quickly.
- Supporting technologies
 - are unreliable
 - do not perform as expected
 - do not work well together where required (i.e., are not interoperable)

3.2.4 Environment Threats

An *environment threat* is an inherent constraint, weakness, or flaw in the overarching operational environment in which a process is conducted. It represents an inherited source of risk,⁸ which makes it difficult to manage in many instances.

⁸ An inherited risk is one that originates outside of a specific entity. For example, a manager overseeing a process might find that his or her mission is at risk due to the actions of partners and collaborators. This is an example of an inherited risk because it originates in parts of the process not controlled by that manager. Likewise, the manager might determine that his or her mission is at risk due to an environment threat, such as lack of cooperation across functional boundaries. Risks caused by environment threats are, by definition, a type of inherited risk because they originate in the overarching operational environment in which a process is conducted.

The following list includes some of the more common environment threats:

- The organization does not reward desired behaviors.
- Organizational lines of authority are not well defined.
- Staff morale is low.
- Organizational politics adversely affect process execution.
- There is lack of cooperation across functional boundaries.
- Communication barriers prevent candid exchanges of information between people throughout the organization.
- Stakeholder pressures adversely affect process execution.
- The physical working environment does not contribute to staff effectiveness.

3.2.5 Event Threats

An *event threat* is a set of circumstances triggered by an unpredictable occurrence that introduces unexpected change into a work process. This unpredictable event must combine with one or more vulnerabilities to produce risk. Typically, these vulnerabilities lie dormant within a work process and do not produce any visible effect on performance during day-to-day operations. However, certain events in combination with these dormant, apparently benign, vulnerabilities place a mission at risk. Examples of event threats include

- surges in workload
- loss of key personnel (management and staff)
- cyber-security breaches
- computer viruses and other types of malicious code
- physical-security breaches
- natural disasters (floods, earthquakes, etc.)
- changes in policies and regulations
- changes in budget and resources
- changes in core mission objectives
- changes in schedule or funding
- introduction of new technology
- changes in customer needs and requirements

The five categories of operational threat thus define a broad range of threats that can put mission success in jeopardy. All threats can be decomposed into two basic elements: (1) a trigger and (2) one or more vulnerabilities. However, there are differences in how threats from different categories arise. The circumstances required to produce an event threat differ from those needed to create threats from the other four categories. In the next section, we

take a closer look at this difference by exploring the underlying mechanics of each threat category.

3.3 Elements of Operational Threat

Table 1 highlights the trigger and vulnerability associated with each category of threat. The table explicitly highlights the fundamental difference between event threats and the other four categories. Whereas an event threat is triggered by an unpredictable occurrence, threats from the other four categories are triggered whenever a work process is executed; no external trigger or occurrence is needed to produce risk. This section explores the specific mechanics of threats, beginning with event threats.

Threat Category	Threat Elements	
	Trigger	Vulnerability
Mission Threat	Process execution	A fundamental flaw, or weaknesses, in the purpose and scope of a work process
Design Threat	Process execution	An inherent weakness in the layout of a work process
Activity Threat	Process execution	A flaw, or weaknesses, arising from the manner in which activities are managed and performed
Environment Threat	Process execution	An inherent constraint, weakness, or flaw in the overarching operational environment in which a process is conducted
Event Threat	Event	Specific vulnerabilities that, when combined with the triggering event, place a mission at risk

Table 1: Elements of Operational Threats

Consider the circumstances that lead to an event threat, such as a computer virus. Many vulnerabilities are embedded in the computer systems that people use every day. Some can affect a computer's performance during routine use by causing it to crash periodically. By contrast, others lie dormant within the computer's operating system and applications and do not produce any visible effect on the computer's performance during day-to-day operations.

A computer virus is a program designed to exploit these dormant vulnerabilities and subsequently cause infected computers to act erratically. People with malicious intent design these programs with the ultimate goal of wreaking havoc throughout the business community. Although there are different types of viruses, which affect computers and their supporting networks in different ways, they typically produce similar results, such as degrading the performance of computers and networks or rendering them unavailable for use. If a work

process is highly dependent on the availability of infected computers and networks, production can be temporarily halted, which puts the work-process mission at risk. Notice that the vulnerability in this example poses no threat to production during typical operating conditions. An unpredictable event, in this case the proliferation of a computer virus, is required for damage to occur.

Now, consider the mechanics of an activity threat. For example, think about what happens when the following vulnerability exists: *inexperienced people, who also have not received adequate training and education for their positions, staff a process*. When asked to perform their assigned tasks, these inexperienced staff members are prone to making mistakes and poor decisions, which puts the work-process mission at risk. Notice that the risk in this example occurs whenever people perform their assignments; no additional trigger is needed. Thus, process execution serves as the trigger that, when combined with certain vulnerabilities, produces a threat. Similar mechanics lead to mission, design, and environment threats.

By reviewing the definitions of each threat category presented in Section 3.2 in relation to the triggers and vulnerabilities from Table 1, you will notice that the definitions provided for the first four categories in the table emphasize vulnerability. For example, the definition of an activity threat is *a flaw, or weaknesses, arising from the manner in which activities are managed and performed*. Notice that this definition focuses exclusively on vulnerability. The trigger (i.e., process execution) is merely implied in the definition.

By contrast, the definition of an event threat is *a set of circumstances triggered by an unpredictable occurrence that introduces unexpected change into a work process*. Notice that this definition focuses on the situation that triggers risk, rather than on the vulnerability that must also be present. In other words, the definition of an event threat implies the existence of vulnerabilities, but does not explicitly mention their existence. This difference is important when expressing and mitigating risk, which we discuss in the next section.

4 Potential Applications

This technical note presents SEI research intended to define the basic structure of risk. We believe that this work will prove to be useful when analyzing the strengths and weaknesses of the risk management methods, tools, and techniques used in today's business environment. We also believe that the ideas presented in this document provide the beginnings of a solid conceptual foundation upon which future risk management work will be based. In this section, we briefly examine two areas in which these concepts can be applied: (1) effective means for communicating risk information and (2) key strategies for mitigating operational risks.

4.1 Expressing Risk

The need to communicate risk information is becoming increasingly important in today's business environment. For example, consider the nature of operational risks that afflict many of today's work processes. Personnel who work most closely with a work process normally have an optimal vantage point for observing its nuances; they understand its shortcomings and flaws. They develop unique insights into how operational risks can adversely affect their abilities to do their jobs. However, they are often unable to manage those risks because they do not usually have sufficient authority to prioritize and allocate mitigation resources. As a result, if these risks are not effectively articulated to management, they cannot be adequately addressed.

All decision makers need to receive timely information about the risks confronting them. The ability to effectively communicate risks and concerns within an organization and across multiple organizations is becoming increasingly important in today's complex business environment. The core elements of operational risk presented in Section 2.5 will influence the requirements for communicating risks. The following items should be considered when communicating risk information:

- *Mission* – Effective communication of operational risk requires all participants to view it within the same context. In other words, people need to have a common understanding of what constitutes success for an operational system. This picture of success must also include an explicit set of criteria for measuring impact and probability.
- *Trigger* – Any expression of operational risk must convey the specific act or event that initiates a given risk. With an event threat, there is uncertainty regarding whether or not the triggering event will occur. That uncertainty is expressed as a probability, which must be included in the expression of risk. With the other four threat categories, there is no uncertainty about the occurrence of their triggers; it is assumed that risk occurs whenever the process is executed.

- *Vulnerabilities* – When expressing operational risk, people must be sure to describe any relevant flaws or weaknesses that expose a work process to potential losses.
- *Impacts* – The potential losses resulting from the occurrence of a risk must also be part of an expression of risk. Each potential impact must also include a value that estimates the extent of prospective losses. In addition, since each potential impact is conditional (meaning that it might or might not occur), all impacts have probabilities associated with them. Those probabilities must also be communicated when articulating risks to others.
- *Controls* – Controls do not always need to be explicitly communicated when discussing risk. However, their effects need to be included in all values of impact and probability.

Note that the above list presents some of the key items to consider when communicating risks to others. However, it does not provide a structured format, or syntax, for expressing risk. Future research will focus on defining a standard structure for conveying risk information to decision makers.

4.2 Mitigating Risk

The core elements of operational risk are also useful for framing mitigation planning activities. For example, common strategies considered during mitigation planning should include the following:

- eliminating a triggering event (applies only to risks resulting from an event threat)
- monitoring for the occurrence of a trigger and implementing contingency plans when appropriate (applies only to risks resulting from an event threat)
- reducing vulnerability
- reducing potential impacts

Notice that this list mirrors the list of controls presented in Section 2.5. Recall that controls include the policies, procedures, practices, conditions, and organizational structures designed to provide reasonable assurance that a mission will be achieved and undesired events will be prevented, detected, and corrected. Risk mitigation strategies are simply means of improving the current set of controls and thus reducing the amount of risk affecting the mission.

Understanding the core elements of risk thus provides a conceptual basis for determining how to mitigate risk.

5 Conclusion

The research presented in this technical note is part of an ongoing body of research in the area of mission assurance. We anticipate that the material in this report will be refined over time as the research progresses. Future publications will reflect any new concepts and philosophies related to risk management and mission assurance.

This body of research began with an effort to consolidate previous research and development activities in the areas of project and security risk management under the banner of operational risk management. The SEI team conducting this research used the Basel II definition of operational risk as a starting point. Recall that the Basel II framework defines operational risk as “the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events” [BIS 04].

Our initial research goal was to define sources of operational risk that are common to most work processes. When cataloging sources of operational risk, team members examined data from risk assessments performed in multiple domains (including software development and organizational security) as well as published references on risk management. We used the following criterion to guide definitions of risk sources: *all threats that could affect completion of an operational mission (i.e., the mission of a work process) must be included in the analysis*. The key outcome of this initial research was the five categories of threat described in Section 3.

We were able to map all threats documented in the reference materials and assessment results into the five threat categories. However, team members also noticed that the five threat categories included sources of risk that went well beyond the Basel II definition of operational risk. At that point, we decided to expand the definition of operational risk to *the potential failure to achieve mission objectives*. This report was written using the team’s revised definition of operational risk.

This technical note marks the completion of the team’s initial phase of work. Based on the results to date, we have decided to take a second look at its decision to expand the definition of operational risk. As we review the definition, we will attempt to answer the following question: *Is the risk triggered by the five categories of threat actually a unique form of risk that is substantially different from operational risk?*

Because the Basel II definition of operational risk is so widely used in the financial community, people within that community might resist adopting the more general definition. At the very least, the general definition of operational risk would likely lead to confusion when presented to a financial audience. As a result, we are considering defining a new form of risk called *mission risk*. Our proposed definition for mission risk is *the possibility that a*

mission might not be successfully achieved. Using the term *mission risk* in lieu of *operational risk* should eliminate any confusion within established communities of practice (e.g., the financial community). As we debate about whether to define this new form of risk, we welcome any feedback or opinions from members of the risk management community.

Finally, identifying the five threat categories has also led us to investigate a broader area of research. It is important to note that the five threat categories are intended to define all major sources of risk that can affect successful completion of a mission. The focus on ensuring mission completion led us to expand our work into the discipline of *mission assurance*, which is an approach for establishing a reasonable degree of confidence in mission success. Mission assurance is achieved when the risk to mission objectives is kept within tolerance. Since the five categories define which threats can put mission objectives at risk, they form the basis for SEI mission assurance research. Future publications will address the topic of mission assurance and examine how it can be used to more effectively manage work processes.

Feedback

The SEI is interested in hearing feedback or opinions from members of the risk management community about the concepts presented here. Please send questions or comments about this technical note to asp-requests@sei.cmu.edu.

References

URLs are valid as of the publication date of this document.

- [Alberts 02]** Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVESM Approach*. Boston, MA: Addison-Wesley, 2002 (ISBN 0-321-11886-3).
- [Alberts 05]** Alberts, Christopher & Dorofee, Audrey. *Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments* (CMU/SEI-2005-TN-032). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.
<http://www.sei.cmu.edu/publications/documents/05.reports/05tn032.html>
- [BIS 04]** Bank for International Settlements (BIS). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. <http://www.bis.org/publ/bcbs107.pdf> (2004).
- [Dorofee 96]** Dorofee, Audrey J.; Walker, Julie A.; Alberts, Christopher J.; Higuera, Ronald P.; Murphy, Richard L.; & Williams, Ray C. *Continuous Risk Management Guidebook*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1996.
<http://www.sei.cmu.edu/publications/books/other-books/crm.guidebk.html>
- [Gallagher 99]** Gallagher, Brian. *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook Version 1.02* (CMU/SEI-99-HB-001, ADA370385). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999.
<http://www.sei.cmu.edu/publications/documents/99.reports/99hb001/99hb001abstract.html>
- [ITGI 00]** IT Governance Institute (ITGI). *COBIT[®] 3rd Edition: Executive Summary*. <http://www.isaca.org/cobit> (2000).
- [Kloman 90]** Kloman, H. F. “Risk Management Agonists.” *Risk Analysis* 10, 2 (June 1990): 201–205.

- [Sharp 01]** Sharp, Alec & McDermott, Patrick. *Workflow Modeling: Tools for Process Improvement and Application Development*. Boston, MA: Artech House, 2001 (ISBN: 1-580-53021-4).
- [Williams 99]** Williams, Ray C.; Pandelios, George J.; & Behrens, Sandra G. *Software Risk Evaluation (SRE) Method Description (Version 2.0)* (CMU/SEI-99-TR-029, ADA001008). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999.
<http://www.sei.cmu.edu/publications/documents/99.reports/99tr029/99tr029abstract.html>
- [Young 01]** Young, Peter C. & Tippins, Steven C. *Managing Business Risk: An Organization-Wide Approach to Risk Management*. New York, NY: American Management Association, 2001 (ISBN: 0-814-40461-8).

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE April 2006		3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE Common Elements of Risk			5. FUNDING NUMBERS FA8721-05-C-0003	
6. AUTHOR(S) Christopher J. Alberts				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213			8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2006-TN-014	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS			12B DISTRIBUTION CODE	
13. ABSTRACT (MAXIMUM 200 WORDS) Traditionally, responsibility for completing a mission and the resources needed to pursue it aligned with organizational boundaries. However, key drivers in the business environment, such as the globalization of business and the fast pace of technological change, have resulted in increased outsourcing and partnering among organizations. It is now common for multiple organizations to work collaboratively in pursuit of a single mission, which creates a degree of programmatic and process complexity that can be difficult to manage effectively. In today's business environment, management and staff must be able to deal with intricate and unclear interrelationships and dependencies among technologies, data, tasks, activities, processes, and people. Mission success in these complex environments requires people to sort through the inherent complexity when making important decisions. Effective risk management that is based on a solid conceptual foundation is an essential part of this decision-making process. This technical note begins to define this foundation by identifying the basic elements of risk and exploring how these elements can affect the potential for mission success.				
14. SUBJECT TERMS assurance, information security, operational system, risk, risk management, risk mitigation, software risk evaluation, risk analysis			15. NUMBER OF PAGES 38	
16. PRICE CODE				
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	